Framework of Cyber Attack Attribution Based on Threat Intelligence

Li Qiang[1,2], Yang Zeming[2], Liu Baoxu[2], Jiang Zhengwei[2(✉)], and Yan Jian[1,2]

[1] University of Chinese Academy of Science, Beijing, People's Republic of China
[2] Institute of Information Engineering, CAS, Beijing, People's Republic of China
{liqiang7, yangzeming, liubaoxu, jiangzhengwei, yanjian}@iie.ac.cn

Abstract. With the rapid growth of information technology, more and more devices are connected to the network. Cyber security environment has become increasingly complicated. In the face of advanced threats, such as targeted attack and advanced persistent threat, traditional security measures of accumulating security devices to protect relevant systems and networks had been proved to be an unqualified failure. Aiming at this situation, this paper proposed a framework of cyber attack attribution based on threat intelligence. At first, after surveying and analyzing related academic research and industry solutions, this paper used the local advantage model to analysis the process of cyber attack. According to the definitions of seven steps in intrusion kill chains and six phases of F2T2EA model, this model proposed a method of collecting threat intelligence data and detecting and response to cyber attacks, so as to achieve the goals of early-warming, processing detection and response and posting attribution analysis, and finally to reverse the security situation. Then, this paper designed a framework of cyber attack attribution based on threat intelligence. The framework is composed by Start of analysis, Threat intelligence and Attribution analysis. The three main parts indicated the architecture of cyber attack attribution. Finally, we tested the framework by practical case. The case study shows that the proposed framework can provide some help in attribution analysis.

Keywords: Cyber attack attribution · Framework · Threat intelligence · Intrusion kill chains · Advanced threat

1 Introduction

With the rapid development of information technology, a huge number of devices connect to the network. Information infrastructure plays key role in business and daily life. In the past, the main security measure was accumulating security devices to protect relevant systems and networks. Ignoring the influence in functions and performances, these security measures had played a certain action in protection of conventional cyber attacks. However, aiming at complex advanced threat, such as targeted attack and advanced persistent threat, the current security measures did not seem to have done as

N. Mitton et al. (Eds.): InterIoT 2016/SaSeIot 2016, LNICST 190, pp. 92–103, 2017.
DOI: 10.1007/978-3-319-52727-7_11

much good as we hoped. An advanced threat refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity [1]. Because these attackers have a certain level of expertise and sufficient resources to conduct their schemes over a long-term period, it is hard to defend and trace advanced threat. For enterprises and governments, advanced threat would lead to harm of reputation or leakage of significant information. Cyber attack attribution analysis is significant.

One definition of cyber attack attribution is "determining the identity or location of an attacker or an attacker's intermediary [2]". According to reconstructing the attack path and the depth and fineness of attack attribution, cyber attack attribution can be divided into four levels [3, 4]: (1) Attribution to the specific hosts involved in the attack, (2) Attribution to the primary controlling host, (3) Attribution to the actual human actor, (4) Attribution to an organization with the specific intent to attack. Effective cyber attack attribution can slow down the paces of attacks. Powerful capacity of attribution is a kind of deterrence [5].

There are several techniques used in cyber attack attribution analysis. Threat intelligence is one of the typical comprehensive methods which we focused on in this paper. According to Gartner definition, threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable device, about an existing or emerging menace or hazard to asset that can be used to inform decisions regarding the subject's response to that menace or hazard [6]. Threat intelligence is based on the collection of intelligence which using open source intelligence, social media intelligence, human intelligence or intelligence in the deep and dark webs. Key mission of threat intelligence is researching and analyzing trends and technical developments in cybercrime, cyber activism and cyber espionage [7]. Threat intelligence is not negate previous security mechanisms, but integrate various security resources to achieve the goals of early-warming, process detection and response and post attribution analysis, and finally to reverse the security situation.

In this paper, we used a local advantage model to deal with cyber attack. This model proposed a method of collecting threat intelligence data and detecting and response to attacks. The goals of cyber attack attribution are early-warming, processing detection and response and posting attribution analysis, and finally reversing the security situation. In order to introduce the process and method of cyber attack attribution analysis, we designed a framework. This framework is mainly composed by the start of analysis, threat intelligence and attribution analysis. Finally, we tested the framework by practical case and got expecting effect.

The main contribution of this paper is proposing a framework for cyber attribution analysis. The framework introduces the processes and components of cyber attack attribution. We also used the designed framework of cyber attack attribution in practical case study. The result shows that the proposed framework can provide some help in cyber attack attribution.

The rest of this paper is organized as follows. The next section describes related work about cyber attack attribution in academic research and industry solutions. Section 3 discusses our research on local advantage model and framework. Section 4 presents a practical case study about cyber attack attribution. Section 5 discusses the

proposed framework and practical case. Section 6 concludes this paper and points out some future research directions.

2 Related Work

2.1 Academic Research

In the research of cyber attack analysis, F2T2EA model [8] was one of the earliest theoretical models which was proposed by United States Air Force and used in intelligence identification, supervision and investigation. The six phases of F2T2EA model are Find, Fix, Track, Target, Engage and Access. During Find step, possible targets are detected and classified for further prosecution. The Fix step of dynamic targeting includes actions to determine the location of the potential target. During Track step, the target is observed and its activity and movement are monitored. During Target step, the decision is made to engage the target in some manner to create desired effects and the means to do so are selected and coordinated. In Engage step, action is taken against the target. The Assessment phase is common to both deliberate and dynamic targeting of the joint targeting cycle and examines the results of the target engagement. United States Department of Defense [9] described the F2T2EA model as the six phases of kill chains in military field, and later it extended to cyber space security.

Lockheed Martin Corporation [10] came up with the intrusion kill chains which are the basic theory of cyber attack attribution analysis. The intrusion kill chains defined seven steps of cyber attack intrusion: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and action on objectives. Reconnaissance means research, identification and selection of targets. Weaponization refers to coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Delivery points Transmission of the weapon to the targeted environment. Exploitation means exploitation triggers intruders' code after the weapon is delivered to victim host. Installation means installation of a remote access Trojan or backdoor on the victim system which allows the adversary to maintain persistence inside the environment. Command and Control (C2) points that compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. Actions on Objectives mean that intruders can take actions to achieve their original objectives after progressing through the first six phases. Those kill chains phases can describe the whole systematic process to target and engage an adversary to create desired effects. The use of threat intelligence is a key component. The indicator is the fundamental element of intelligence in this model.

Sergio Catagirone [11] proposed a diamond model expected to add the cost of cyber attack and decrease the cost of defender. Diamond model provides a method to integrate the intelligence for analysis platform and make correlation, classification and forecast based on activities of attackers. The basic element of diamond model is event. Each event composed of four core features: adversary, capability, infrastructure and victim. These features are edge-connected representing their underlying relationships and arranged in the shape of a diamond. These elements, the event, thread, and group

all contribute to a foundational and comprehensive model of intrusion activity built around analytic processes.

Thomas Rid [12] proposed a Q model designed to explain, guide, and improve the attribution. The paper holds the opinion that matching an offender to an offence is an exercise in minimizing uncertainty on three levels: tactically, attribution is an art as well as a science; operationally, attribution is a nuanced process not a black-and-white problem; and strategically, attribution is a function of what is at stake politically. Successful attribution requires a range of skills on all levels, careful management, time, leadership, stress-testing, prudent communication, and recognizing limitations and challenges.

The above models and methods mostly were proposed for specific requirements in specific scenarios, so there are some differences in research fields and focuses. This paper discussed the framework of cyber attack attribution based on threat intelligence. The discussed models and methods can provide some references in idea and research methods, especially F2T2EA model and intrusion kill chains.

2.2 Industry Solutions

In the industry of cyber security, there are several solutions aimed at cyber attack. Owning over 300 million users and over 250000 corporate clients worldwide, Kaspersky Lab [13] has powerful malware analysis ability which has over more than 1000 research and development experts, especially the Global Research and Analysis Team (GReAT) established in 2008. GReAT is an elite group of recognized cyber security experts located around the globe and bring local expertise and threat intelligence to monitor the world threat landscape. Till now, GReAT had discovered many sophisticated threats and release relevant APT intelligence reports, like Duqu, Flame, Gauss, Red October, etc [14].

FireEye [15] is a publicly listed us network security company which founded in 2004. The FireEye Intelligence Center provides access to strategic intelligence, analysis tools, intelligence sharing capabilities, and institutional knowledge based on over 10 years of FireEye and Mandiant experience detecting, responding to and tracking advanced threats. FireEye's intelligence databases can provide real-time, actionable intelligence analytical ability which is a patented 115+ million node graph-based engine with 340 million defined relationships, 600 terabytes of storage and over 500+ million reviewed network streams. Till now, FireEye has proposed several influential APT analysis reports, like APT1, APT28, APT30, etc [16].

Dell SecureWorks [17] proposed the security integration method from core asset to service and business value. They develop the counter threat platform which is at the core of intelligence-driven information security solutions. The counter threat platform [18] can analyze more than 160 billion network events to discover potential threats, deliver countermeasures and generate intelligence and valuable context regarding the intentions and actions of adversaries.

IBM X-Force Research and Development [19] is one of the most renowned commercial security research and development teams in the world. These security professionals monitor and analyze security issues from a variety of sources, including its

database of more than 96,000 computer security vulnerabilities, its global web crawler can collect and detect over 25 B catalogued web pages and URLS, and millions of malware samples daily.

The above industry solutions are is focusing on the deployment and implement of business. They mostly used threat intelligence as an effective technology in malware analysis and cyber attack detection and attribution. In view of business secrets, the introduction of industry solutions excludes detailed information about framework and content, but it can provide some ideas and references, especially the technical solution and implement.

3 Our Research

According to the reference of related work and the actual situation, we used the local advantage model [20] to make full use of threat intelligence data from kinds of self-building security platforms and external channels to achieve the goals of early-warming, process detection and response and post attribution analysis. We also designed a framework of cyber attack attribution to solve the hardship in cyber attack analysis. Detail introductions are shown as follows.

3.1 Local Advantage Model

According to the definitions of seven steps in kill chains and six phases of F2T2EA model, the deployed continuous monitoring platform can collect kinds of attack related information to find and fix cyber attack. The useful information can be regard as the source of threat intelligence platform. By making full of threat intelligence information, the output knowledge can be used to track and target the attackers, and also can be seem as the input of comprehensive response platform to engage and assess the security systems and information infrastructure. Considering about this, we used a model to get local advantage in cyber security situation. The model is shown in Fig. 1.

In Find step of this model, we can get helpful information from suspicious alarm, vulnerability disclosure, NIDS (Network Intrusion Detection System), abnormal behavior detection, malware detection, threat intelligence platform and audit log during the seven phases of kill chains. In Fix step, security reinforce scheme refers to assets vulnerability management, NIDS, malware alarm, active report and abnormal behavior alarm, etc. In order to track and target the attackers, we can use flow analysis, log analysis, reverse analysis, trace back, honeypot and expert analysis, etc. In Engage step, responses and solutions include: black and white list, vulnerability mending, IPS (Intrusion Prevention System), anti-malware, DEP (Data Execution Prevention), process and authority protection, DNS redirect filtering, internal intrusion block, and forensic, etc. In final Assess step, assess measures need to be taken, including damage evaluation, threat intelligence sharing, emergency response drill, security education and training, management flow optimization and protection mechanism adjustment, etc.

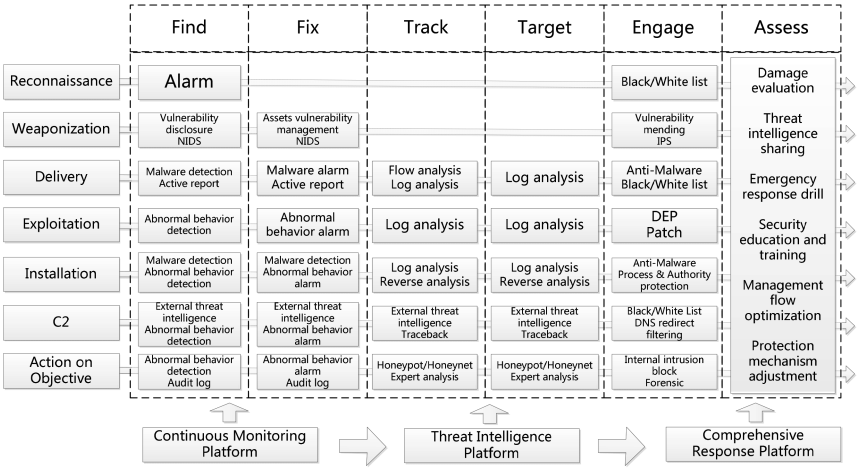

Fig. 1. Local advantage model based on threat intelligence

3.2 Framework of Cyber Attack Attribution

The framework of cyber attack attribution is used to describe the analysis procedure, platform construction and analysis content of cyber attack attribution. What's more, this framework can be regarded as the reference for schema design of actual deployment. The component of framework includes the start of analysis, the standard of threat intelligence, relevant data and systems of threat intelligence, evaluation of threat

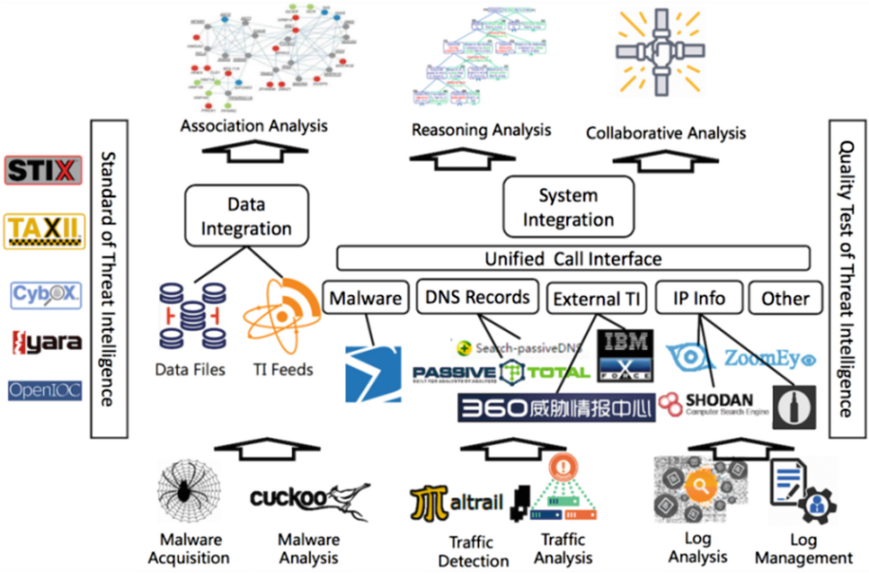

Fig. 2. Framework of cyber attack attribution

intelligence data and cyber attack attribution analysis. Figure 2 illustrates the framework of cyber attack attribution.

The framework is consists of three main parts: start of analysis, threat intelligence and attribution analysis. The internal components of every framework part and functionalities are discussed in the following:

(1) Start of analysis

According to the experience of emergency response and cyber-attack analysis, the original data mainly consist of three aspects: malware samples, network traffic and log records. In the course of the experiment, we can get malware from malware sample websites by web spider. Malware sandbox can be used to analyze the malicious activities of malwares, such as Cuckoo and ZeroWine, etc. Traffic detection and analysis are the main task of network traffic analysis. We can add evil IP address and domain name to black list to detect malicious behaviors. The association relation among the traffic data can be found by traffic analysis. Typical traffic detection and analysis software include Wireshark, Moloch, Malcon and Maltrail, etc. The tasks related to log include log management and analysis. The log records may contain users' access history, alarm information and operating records, etc. Powerful log management can provide effective in log analysis. Malware samples, network traffic and log records are the start of cyber attack attribution analysis.

(2) Threat intelligence

The task related to threat intelligence includes standard of threat intelligence, data integration, system integration and quality test of threat intelligence. Typical standards of threat intelligence include STIX (Structured Threat Information Expression), TAXII (Trusted Automated eXchange of Indicator Information), CybOX (Cyber Observable Expression), Yara and OpenIOC, etc. we can use and reference these standards in practical work of attribution analysis. Threat intelligence data integration means integrating various data files and threat intelligence feeds data to center database. System integration points that using unified call interface to integrate different kinds of systems, including malware detection system (e.g. VirusTotal), Passive DNS record system (e.g. Qihoo 360 Passive DNS, Passive Total), External threat intelligence platform (e.g. Qihoo 360 Threat Intelligence, IBM xForce.), IP related information (e.g. ZoomEye, Shodan, IVRE) and other related systems. Through system integration, we can make full use of threat intelligence in attribution analysis. Quality test of threat intelligence is to evaluate the quality of threat intelligence date from exchange of threat intelligence to get better analysis result. Threat intelligence is the basis of cyber attack attribution.

(3) Attribution analysis

Threat intelligence data is the input of attribution analysis. There are three kinds of attribution analysis methods: association analysis, reasoning analysis and collaborative analysis. Association analysis is to get as more as relevant and important data from threat intelligence database. Constraint and efficiency are the main concerns in the process of association analysis. Reasoning analysis is to get the possible relationship and attack chains from the associated data. The target of collaborative analysis is

making full use of the performance of computer and the thinking of analysts in attribution analysis. Analysis is the main task in the process of cyber attack attribution.

This framework introduced the architecture of cyber attack attribution from the start of analysis to threat intelligence and analysis. From the framework, we can find out the process of cyber attack attribution and the related information and systems. At the same time, according to the framework, we can quickly build a testing environment to evaluate the effort of cyber attack attribution.

4 Case Study

In order to introduce the process and the framework of cyber attack attribution analysis, we used a practical case of cyber attack as follow. During the two meetings of China, there was a government website X had been attacked and some webpages had been distorted. Aiming at this situation, we started to investigate and analyze. The survey result shows that this organized attack was likely to be a targeted attack. The analysis processes are shown as follows:

(1) Website X had been attacked and its webpages had been distorted to objectionable content. We started the investigation and analysis.
(2) After detected the website and relevant severs, and analyzed the log files, we found that the website existed several vulnerabilities of Struct2 and SQL injection. We also found two suspicious executable files named "jpublish" and "syslogd" in server hosts. Their MD5 values are "d41d8cd98f00b204e9800998ecf8427e" and "4f1c0a24761deb8fd95e467add18a97f".
(3) At the same time, there were several severs exist more than two IP connections. Through network traffic capturing and analysis, we got two suspicious IP addresses: 122.10.41.105 and 122.10.13.99.
(4) By using the passive DNS systems integrated in threat intelligence platform, we reversely parsed the IP address and got the records. We can get the information about domain name, parsing type and the last parsing time. The parsing records are shown in Tables 1 and 2.
(5) According to registration related information of domain, we made an association analysis among these information data. Through the two IP addresses, we can find lot of possible associated information from threat intelligence data. Association graph is shown in Fig. 3.

Table 1. 122.10.13.99 parsing records

Domain	Type	Time
jbp567.com	A	2015-03-20 18:11:11
www.jbp234.com	A	2015-03-21 23:17:47
www.cp-cp.cc	A	2015-03-01 00:02:47
jbp234.com	A	2015-03-21 20:11:10
www.jbp345.com	A	2015-03-01 21:31:35
tt80001.com	A	2016-03-10 13:29:54

Table 2. 122.10.41.105 parsing records

Domain	Type	Time
caiyuanbc.com	A	2015-06-16 16:04:30
www.caiyuan1688.com	A	2015-06-03 16:13:41
www.zcedez.com	A	2015-09-21 14:05:06
www.bcpingji588.com	A	2015-09-30 07:41:43
www.osoomo.com	A	2015-09-08 10:13:59
ibaijiale.wang	A	2015-06-30 14:24:18
admin.skws4.dwmdph.com	A	2015-09-08 14:07:05
www.kpuduk.com	A	2015-09-08 00:19:06
www.zcogsz.com	A	2015-09-07 12:32:30
www.kqnhqb.com	A	2015-09-07 12:03:55
bak.888888k.com	A	2015-09-07 12:03:55
umikl.com	A	2010-03-55 12:57:48

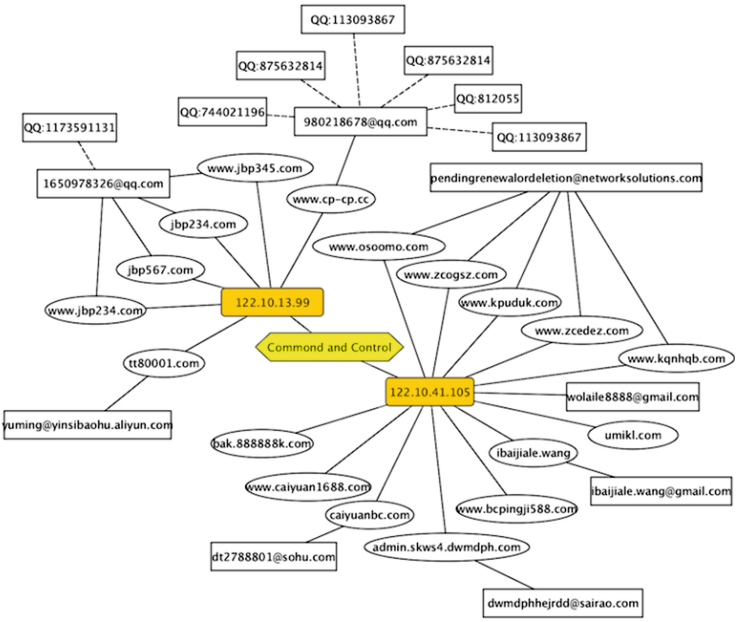

Fig. 3. Association graph

(6) By utilizing associated information in threat intelligence platform, we also built an association by STIX model. Through the STIX associated graph, we can clearly find out the attackers and attack process related information. The threat intelligence associated graph is shown in Fig. 4.

(7) By mapping the attack related information to the seven phases of kill chains and reasoning and supplying the miss clue and association, we can describe a

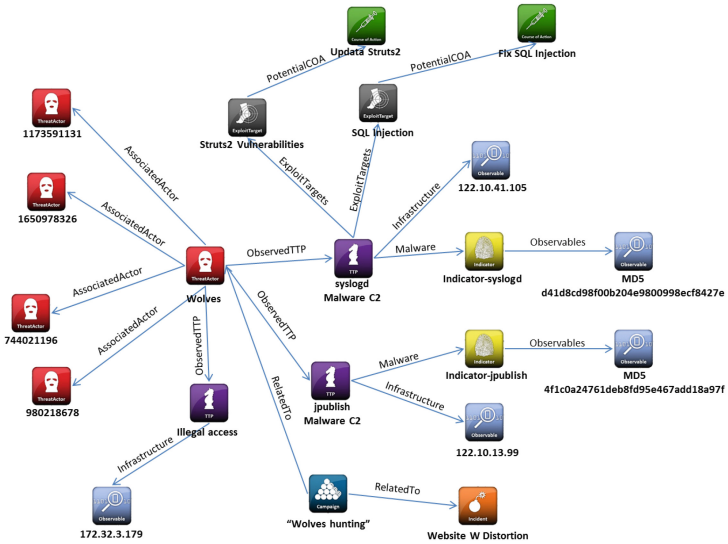

Fig. 4. Threat intelligence associated graph by STIX model

complete attack process. The parts with underline mean the reasoning and supplementing clues. The red dash arrow line means the association by reasoning. The red arrow line means mean the association by existing evidence. In this case, we found three suspicious threads in the whole attack process after analyzing and reasoning by the framework. The whole mapping and reasoning process is shown in Fig. 5.

Phase	Thread1	Thread2	Thread3
Reconnaissance	Scanning and detection		
Weaponization	Develop exploiting application Prepare exploit code		
Delivery	Webshell		IP:172.32.3.179
Exploitation	Struts2 vulnerabilities SQL injection		Privilege vulnerabilities
Installation	Jpublish	syslogd	
C2	122.10.13.99 [Heartbeat packets]	122.10.41.105 [Heartbeat packets]	
Action on Objectives	Website Distortion		Illegal Access

Fig. 5. Whole mapping and reasoning process.

5 Discussion

The main research content in this paper is the framework of cyber attack attribution. The theoretical basis of this framework is local advantage model. Through analyzing local advantage model, we can get the whole process of cyber attack and the related data in each stage. So we firstly researched existing models on cyber attack attribution analysis. Considering that the framework tends to the practical application, we subsequently researched industry solutions. Finally we determined to use threat intelligence in cyber attack attribution.

Because the detailed content of local advantage model and technology used in the framework are not the key points in this paper, we discussed little about them. In order to understand the process of cyber attack attribution based on threat intelligence, the paper combines the analysis of actual cases, so as to enhance the practical application of this value. The result of case study shows that the proposed framework can provide some help in cyber attack attribution analysis.

6 Conclusion and Future Works

According to the situation that current main security measures are accumulating security devices to protect relevant systems and networks, but the efforts is dissatisfied for advanced threats, we used an advantage model based on threat intelligence to deal with cyber attack. This model made full use of the constructed continuous monitoring platform, threat intelligence platform and comprehensive response platform to achieve the goals of early-warming, process detection and response and post attribution analysis through the seven steps of intrusion kill chains, and finally to reverse the security situation. We also came up with a framework of cyber attack attribution to describe the whole process of analysis. The framework introduced the related actions and resources in attribution analysis, including the start of analysis, the standard of threat intelligence, related data and systems of threat intelligence. Finally, we tested the model and framework by practical case. The case study indicated that the proposed framework and corresponding testing environment can provide some help in cyber attack attribution analysis. Framework of cyber attack attribution based on threat intelligence would be an effective architecture for cyber attack attribution.

In the future, our main energy focused on detailed technology and implements, especially automated analysis. Full-automated analysis would make full use of the advantage of threat intelligence data and platform, which could play an important role in cyber attack attribution analysis.

References

1. Trend Micro. Targetted Attacks (2016). http://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks
2. Wheeler, D.A., Larsen, G.N.: Techniques for cyber attack attribution. No. IDA-P-3792. Institute for Defense Analyses, Alexandria, VA (2003)
3. Ryu, J., Na, J.: Security requirement for cyber attack traceback. In: Fourth International Conference on Networked Computing and Advanced Information Management, NCM 2008, vol. 2. IEEE (2008)
4. Hunker, J., Hutchinson, B., Margulies, J.: Role and challenges for sufficient cyber-attack attribution. In: Institute for Information Infrastructure Protection, pp. 5–10 (2008)
5. Tony Code. Attributions and Arrests: Lessons from Chinese Hacker (2015). https://www.fireeye.com/blog/executive-perspective/2015/12/attributions_andarr.html
6. Gartner. Definition: Threat Intelligence (2013). https://www.gartner.com/doc/2487216/definition-threat-intelligence
7. Gervais, P.: Nine Cyber Security Trends for 2016 (2015). http://www.prweb.com/releases/2015/12/prweb13125922.htm
8. Tirpak, J.A.: Find, fix, track, target, engage, assess. Air Force Mag. **83**(7), 24–29 (2000)
9. U.S. Department of Defence. Joint Publication 3-60 Joint Targeting (2007). http://www.bits.de/NRANEU/others/jp-doctrine/jp3_60(07).pdf
10. Hutchins, E.M., Cloppert, M.J., Amin, R.M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: Leading Issues in Information Warfare and Security Research, vol. 1, p. 80 (2011)
11. Caltagirone, S., Pendergast, A., Betz, C.: The diamond model of intrusion analysis. In: Center for Cyber Intelligence Analysis and Threat Research, Hanover, MD (2013)
12. Rid, T., Buchanan, B.: Attributing cyber attacks. J. Strateg. Stud. **38**(1-2), 4–37 (2015)
13. Kaspersky. Kaspersky Lab Technology Leadership (2014). http://www.kaspersky.com/other/custom-html/b2b-ddos-prevention/pdf/kaspersky-technology-leadership.pdf
14. Kaspersky. Kaspersky Security Intelligence Services (2014). http://media.kaspersky.com/en/business-security/enterprise/Kaspersky_Security_Intelligence_Services_Threat_Intelligence_Services.pdf
15. FireEye. FireEye Threat Intelligence Engine (2015). https://www.fireeye.com/products/dynamic-threat-intelligence/threat-intelligence-engine.html
16. FireEye. FireEye Intelligence Center (2015). https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/ds-fireeye-intelligence-center.pdf
17. Dell SecureWorks. Ever-Evolving Security Threat Landscape (2014). http://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/ISACAATL-062014-EverevolvingSecurityThreatLandscape.pdf
18. Dell SecureWorks. Counter Threat Platform (2016). https://www.secureworks.com/capabilities/counter-threat-platform
19. IBM Security. IBM X-Force Threat Intelligence (2016). http://www-03.ibm.com/security/xforce/
20. Qiang, L., et al.: A reasoning method of cyber-attack attribution based on threat intelligence. World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng. **10**(5), 773–777 (2016)